Hewlett Packard Enterprise

HPE 3PAR OS 3.3.1 MU2 Patch 51 Release Notes

Abstract

This release notes document is for 3.3.1 MU2 Patch 51.

Part Number: QL226-10581a
Published: February 2019
Edition: 2

Acknowledgements

Microsoft and Windows are U.S. registered trademarks of Microsoft Corporation.

Adobe® and Acrobat® are trademarks of Adobe Systems Incorporated.

Java and Oracle are registered trademarks of Oracle and/or its affiliates.

UNIX® is a registered trademark of The Open Group.

Intel®, Itanium®, Pentium®, Intel Inside®, and the Intel Inside logo are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Purpose

The HPE 3PAR OS 3.3.1 MU2 Patch 51 provides several critical quality improvements.

IMPORTANT: See the **HPE 3PAR OS and Service Processor Software Update Guide (HPE 3PAR OS 3.3.1 HPE 3PAR Service Processor 5.x)** for instructions on updating your specific software.

Guidance

This is a critical patch.

IMPORTANT: Do not install this patch on arrays where the File Persona component version is 1.5, and File Persona is in use with File Provisioning Groups configured for Remote Copy. For those systems, wait for an upcoming File Persona patch, which will include Patch 51.

Prerequisites

- Minimum Service Processor required: 5.0.3 + latest SP patch.
- Base OS: 3.3.1 MU2. See the Requires field in the Patch details.

Patch details

Patch ID: P51

Synopsis: Provides several critical quality improvements

Date: February 08, 2019, 11:33:08 PST

Description: See the Release Notes for details about this patch

Affected Packages: tpd-cli, tpd-fipsvr, tpd-kernelpatch, tpd-libcli, tpd-libcomm, tpd-pr, tpd-qw, tpd-sysmgr, tpd-prerevert

Obsoletes: OS-3.3.1.410-P48

Requires: OS-3.3.1.410-MU2

Build Version: 3.3.1.514

Patches Included: OS-3.3.1.410-P32,OS-3.3.1.410-P40,OS-3.3.1.410-P45

Patches Partially Superseded: OS-3.3.1.410-P32,OS-3.3.1.410-P40,OS-3.3.1.410-P45

Patches Obsolete by Combination: None.

Supports Revert: Yes

Notes: Description of the obsoleted patches:

Patch ID: P48

Synopsis: Further improves error handling for certain drive models.

Date: December 11, 2018, 22:53:16 PST

Description: See the Release Notes for details about this patch.

Affected Packages: tpd-kernelpatch, tpd-libcli, tpd-sysmgr, tpd-prerevert

Obsoletes: OS-3.3.1.410-P46

Requires: OS-3.3.1.410-MU2

Build Version: 3.3.1.497

Notes: Description of the obsoleted patches:

Patch ID: P46

Synopsis: Improves array cluster validation process

Date: December 10, 2018, 15:30:51 PST

Description: See the Release Notes for details about this patch.

Affected Packages: tpd-kernelpatch, tpd-prerevert

Obsoletes: None

Requires: OS-3.3.1.410-MU2,OS-3.3.1.410-P30,OS-3.3.1.410-P32,OS-3.3.1.410-P40,OS-3.3.1.410-P45

Build Version: 3.3.1.496

Notes:

NOTE:

Hewlett Packard Enterprise recommends installing patches in the same sequence as they are released, unless instructed otherwise.

Patches Included in This Release

HPE 3PAR OS 3.3.1 MU2 P51 includes the following patches.

NOTE: To learn more about each patch, use the links provided to access the individual patch release notes.

Patch	Description	Obsoletes	Links to Documentation
HPE 3PAR OS 3.3.1 MU2 Patch 32	Provides several critical quality improvements.	None.	**https://support.hpe.com/hpsc/doc/public/display?docId=emr_na-a00051930en_us**
HPE 3PAR OS 3.3.1 MU2 Patch 40	Provides several critical quality improvements.	OS-3.3.1.410-P30,OS-3.3.1.410-P38	**https://support.hpe.com/hpsc/doc/public/display?docId=emr_na-a00057833en_us**
HPE 3PAR OS 3.3.1 MU2 Patch 45	Provides several critical quality improvements.	None.	**https://support.hpe.com/hpsc/doc/public/display?docId=emr_na-a00059979en_us**

Modifications

HPE 3PAR Patch 51 addresses the following issues:

Issue ID: 252554, 247254, 246894

Issue summary: **`setsys DisableCompr no`** cannot be used to enable compression after it has been disabled.

Platforms affected: StoreServ 8000, StoreServ 9000, StoreServ 20000

Affected software versions: 3.3.1 GA - MU3

Issue description: **`setsys DisableCompr no`** cannot be used to enable compression after it has been disabled without re-initializing the array.

Symptoms: Unable to turn on compression using **`setsys`**.

Conditions of occurrence: CLI command **`setsys DisableCompr yes`** has been issued

Impact: Medium

Customer circumvention: Do not disable compression with **`setsys DisableCompr yes`**.

Customer recovery steps: None.

Issue ID: 245261

Issue summary: Communication with External Key Management servers (EKMs) does not work correctly if more than two EKMs are defined.

Platforms affected: All StoreServ

Affected software versions: 3.2.2 GA - MU6, 3.3.1 GA - MU2

Issue description: When more than two External Key Management servers are defined, the array will only successfully communicate with the first configured EKM. This situation will result in the array being unable to retrieve a key when the primary EKM is unreachable, and rekey operations will not successfully complete.

Symptoms: Encryption keys will not be retrieved if the more than two EKMs are defined and the primary EKM is unreachable.

Encryption rekey operations will not successfully complete if more than two EKMs are defined.

Conditions of occurrence: More than two EKMs are defined.

Impact: High

Customer circumvention: Reduce the number of configured EKMs to two.

Customer recovery steps: Restore connection to primary EKM or contact support to provide a backup file with different EKMs defined.

Issue ID: 226214, 250186, 250189, 227826, 225250, 239105

Issue summary: Slow management response times during `InSplore` collection.

Platforms affected: All StoreServ

Affected software versions: 3.3.1 GA - MU2

Issue description: In version 3.3.1, with SP 5.x.x, `InSplore` data is collected internally to the array before being copied off by the SP. The data gathering process can be time consuming and affect other array processes.

Symptoms: Slow management response times during `InSplore` collection.

Conditions of occurrence: `InSplore` collection is being done during heavy usage times.

Impact: Low

Customer circumvention: Avoid `InSplore` collection during heavy array usage times.

Customer recovery steps: None.

Issue ID: 237143, 251701

Issue summary: Data becomes unavailable during controller node down recovery.

Affected platforms: All StoreServ

Affected software versions: All

Issue description: When one controller node is in controller node down recovery, one of the other controller nodes tries an interprocess communication (IPC) request and does not succeed. This causes all the controller nodes to unexpectedly restart resulting in data unavailability.

Symptoms: Data becomes unavailable during controller node down processing.

Conditions of occurrence: During a controller node down recovery, one of the other controller nodes retries an IPC request. A response is received before the send request is completed.

Impact: High

Customer circumvention: None.

Customer recovery steps: None.

Issue ID: 244667

Issue summary: Peer Motion Migrations for Windows Clusters may result in data becoming unavailable.

Platforms affected: All StoreServ

Affected software versions: 3.3.1 GA - MU3

Issue description: During Windows Cluster Peer Motion Migrations on 3.3.1, data may become unavailable when I/O from the Windows Cluster encounters a SCSI-3 reservation conflict from the source array.

Symptoms: Data unavailable.

Conditions of occurrence: Peer Motion Migration of Windows Cluster storage when array is running HPE 3PAR OS 3.3.1.

Impact: High

Customer circumvention: Perform Peer Motion during downtime for Windows Cluster.

Customer recovery steps: None.

Issue ID: 254203, 247571, 233388

Issue summary: A fibre channel Discover Address (**`ADISC`**) request does not respond, and creates an unwanted callback invocation.

Platforms affected: All StoreServ

Affected software versions: 3.2.2 MU4 - MU6, 3.3.1 GA - MU3

Issue description: Utility for orphaning Extended Link Services (ELS) request bypasses a `Dev Lost` scenario. This results in an unwanted callback invocation from a timed out **`ADISC`** request.

Symptoms: Single controller node restart.

Conditions of occurrence: 16G/32G Fibre Channel driver is being used.

Impact: Medium

Customer circumvention: None.

Customer recovery steps: None.

Issue ID: 215766, 213320, 251621

Issue summary: Unable to perform any maintenance tasks when internal table backups are overextended.

Platforms affected: All StoreServ

Affected software versions: All

Issue description: The array's internal table data backup mechanism is overextended. This situation can lead to the array becoming unresponsive to administrative tasks and to data becoming unavailable.

Symptoms: CLI commands on the array become unresponsive.

Event log entries are not recorded.

Administrative actions will not complete.

Conditions of occurrence: The array's internal mechanism for backing up table data becomes overextended and slow to respond.

Impact: Medium

Customer circumvention: None.

Customer recovery steps: None.

Issue ID: 199872, 251564, 251565

Issue summary: Unable to create snapshot administration logical disks with **`-ha mag`**.

Platforms affected: All StoreServ

Affected software versions: 3.2.2, 3.3.1 GA - MU3

Issue description: Unable to create snapshot administration logical disks with **`-ha mag`** if free space left in one cage only out of three or more cages per controller node pair.

Symptoms: Unable to grow snapshot administration space.

Conditions of occurrence: If there are three or more cages attached per controller node pair and all full except one cage, the **`createald`** command will not able to create snapshot administration logical disks with **`-ha mag`**.

Impact: Medium

Customer circumvention: Balance chunklet usage across the physical disk cages.

Customer recovery steps: Add **`-ssz 3`** for snapshot administration space in the common provisioning group parameter.

Issue ID: 221871, 249619, 251649, 251650

Issue summary: The array unexpectedly restarts when trying to access an inconsistent compression volume page.

Platforms affected: All StoreServ

Affected software versions: 3.3.1 GA - MU2

Issue description: If a compression volume page is inconsistent, the array restarts when a defragmentation process is trying to access the inconsistent page.

Symptoms: The array restarts at the same interval as the defragmentation schedule.

Conditions of occurrence: Array running 3.3.1 GA or 3.3.1 MU1 or 3.3.1 MU2 with compression volumes, where one or more volumes contains an inconsistent page.

Impact: High

Customer circumvention: None.

Customer recovery steps: None.

Issue ID: 250754, 237546, 249619, 235371, 251482

Issue summary: Virtual Volume checks do not run after powerfail wipe with `n-1` recovery.

Platforms affected: All StoreServ

Affected software versions: 3.3.1 GA - MU2

Issue description: Repeated restarts in powerfail recovery cause the powerfail data to be removed. Virtual Volume checks are incorrectly marked as being done. This leaves inconsistencies in the metadata that cause controller nodes to unexpectedly restart.

Symptoms: Virtual volume checks do not run.

Conditions of occurrence: Enter powerfail recovery attempting to do `n-1` recovery.

Impact: High

Customer circumvention: None.

Customer recovery steps: Take the volumes offline and perform logical disk checks and VV checks. This includes bringing entire deduplication groups offline to perform group **`checkvv`**. **`sdmetack`** is also required after these steps for compressed volumes.

Issue ID: 250237

Issue summary: Controller node restarts upon race condition between two processes.

Platforms affected: All StoreServ

Affected software versions: 3.3.1 GA - MU2

Issue description: Unplanned controller node restarts occur upon a race condition between two processes. These restarts occur in the presence of compressed deduplicated volumes with Read Only (RO) or Read Write (RW) snaps which have had the **`updatevv`** operation run on them.

Symptoms: Controller node unexpectedly restarts.

Conditions of occurrence: Presence of compressed deduplicated volumes with snapshots and **`updatevv`** operation performed on them anytime prior.

Impact: Medium

Customer circumvention: None.

Customer recovery steps: None.

Issue ID: 255132, 255133, 248022, 247631

Issue summary: Duplicate session alerts cause unexpected controller node restarts.

Platforms affected: All StoreServ

Affected software versions: 3.2.2 MU6, 3.3.1 GA - MU3

Issue description: Duplicate logins from the iSCSI initiators cause duplicate session alerts. The event logging subsystem allocates memory for these alerts and eventually runs out of memory.

Symptoms: Controller node unexpectedly restarts.

Conditions of occurrence: Duplicate sessions from the initiators.

Impact: Medium

Customer circumvention: None.

Customer recovery steps: None.

Issue ID: 243157, 243105

Issue summary: When all Remote Copy links are down, Virtual Volumes belonging to synchronous Remote Copy groups are temporarily put in an Asymmetric Logical Unit Access (ALUA) transition state.

Platforms affected: All StoreServ

Affected software versions: 3.2.2 MU2 - MU6, 3.3.1 MU1 - MU3

Issue description: When all Remote Copy links are down, Virtual Volumes (VVs) belonging to synchronous Remote Copy groups are temporarily put in an Asymmetric Logical Unit Access (ALUA) transition state. If System Manager restarts, the VVs may remain in a transition state, resulting in data becoming unavailable. VVs will no longer be in transition state.

Symptoms: Data becomes unavailable.

Conditions of occurrence: System Manager and controller node restart after all Remote Copy links are down and VVs belong to Remote Copy sync group are in transition state.

Impact: High

Customer circumvention: None.

Customer recovery steps: Check the VVs which are in transition state. **`showvlun`** will show them, if the exported host is online. Ensure that the affected groups are not in failed-over/failsafe state. For each VV/VLUN which is stuck at ALUA transition state which is part of Remote Copy group, run the **`setvv -setalua 0 <vv_name>`** command.

Issue ID: 160853, 198379, 214647, 217390, 226158

Issue summary: A single controller node restarts.

Platforms affected: All StoreServ

Affected software versions: 3.2.2 MU1 - MU6, 3.3.1 GA - MU3

Issue description: Two threads working on the same cache memory page cause a single controller node to restart.

Symptoms: A single controller node restarts.

Conditions of occurrence: Normal operation.

Impact: Medium

Customer circumvention: None.

Customer recovery steps: None.

Issue ID: 250806, 237618

Issue summary: Accessing stale metadata causes the controller node to restart.

accessing causing a controller node restart

Platforms affected: All StoreServ

Affected software versions: 3.3.1 GA - MU2

Issue description: Accessing stale metadata creates a race condition between two different I/O requests. This condition leads to a controller node restarting.

Symptoms: Controller node restarts.

Conditions of occurrence: Normal operation.

Impact: Medium

Customer circumvention: None.

Customer recovery steps: None.

Issue ID: 252572, 252564, 247853, 212271, 252571

Issue summary: Quorum Witness configured with an IPV6 address gets reset by System Manager if the network connection between the administrator controller node and the Quorum Witness is less than optimal.

Platforms affected: All StoreServ

Affected software versions: 3.3.1 GA - MU3

Issue description: When configured with IPV6 addresses, if the network latencies between the administrator controller node and the Quorum Witness are high, bursts of connection issues force System Manager to reset Quorum Witness. A quorum reset can be disruptive because it cannot be used to inform an automatic failover decision if the RC target happens to fail at the same time.

Symptoms: Bursts of Quorum Witness unreachable events.

Conditions of occurrence: Quorum Witness is configured with IPV6 addresses.

Impact: High

Customer circumvention: Avoid high latencies between array controller nodes and Quorum Witness.

Customer recovery steps: None.

Issue ID: 234624, 243677

Issue summary: While using Peer Persistence or Remote Copy, the primary will check the link state. If a transient Quorum Witness communication error is received while checking the link state, it results in failsafe action causing data to become unavailable.

Platforms affected: All StoreServ

Affected software versions: 3.2.2 GA - MU6, 3.3.1 GA - MU4

Issue description: In a system configured with Peer persistence, a target failure check transient Quorum Witness communication error is received. This condition results in failsafe action, causing data to become unavailable.

Symptoms: Virtual Volumes affected by failsafe experience data unavailability.

Conditions of occurrence: The array is configured with peer persistence and Quorum Witness.

Impact: High

Customer circumvention: None.

Customer recovery steps: Use the override option to bring volumes out of failsafe state.

Issue ID: 214117, 219015, 245809, 245822

Issue summary: `MC_CHECK_CONSISTENCY` alert.

Platforms affected: All StoreServ

Affected software versions: 3.3.1 MU2

Issue description: Event log shows `Configuration lock hold time` alerts. Volume checks have longer run times, leading to extraneous alerts reported by System Manager's call monitor.

Symptoms: An `MC_CHECK_CONSISTENCY` alert appears.

Conditions of occurrence: Normal operation.

Impact: Low

Customer circumvention: None.

Customer recovery steps: Remove the alert.

Issue ID: 230407, 234150, 183091, 154837

Issue summary: The array restarts unexpectedly if Flash Cache simulation is enabled during an upgrade, or while the System Manager restarts.

Platforms affected: All StoreServ

Affected software versions: 3.3.1 MU1 - MU2

Issue description: If Flash Cache simulation is enabled either during upgrade, or if System Manager restarts, there is an unwanted increase in memory usage. This increase leads to array `Out of Memory` situation and eventually the array restarts.

Symptoms: Array physical memory (RAM) usage increases in an incremental fashion. Each time System Manager is restarted, or during an upgrade, approximately 800 MB of memory space which is not reclaimed. After several restarts, the array reaches its full memory capacity and restarts.

Conditions of occurrence: Flash Cache simulation is enabled. Either System Manager restarts, or an upgrade is performed.

Impact: High

Customer circumvention: Disable Flash Cache simulation before performing an upgrade.

Customer recovery steps: None.

Issue ID: 253308, 236286

Issue summary: Input/output commands time out due to collision of the SCSI **`GET_VVMAP`** command and creation of the snapshot.

Platforms affected: All StoreServ

Affected software versions: 3.2.2, 3.3.1 GA - MU2

Issue description: The incremental backup job hangs due to inter-node deadlock when a **`GET_VVMAP`** command interrupts before snapshots have been fully defined.

Symptoms: Input/output commands time out. The array becomes unresponsive to commands, and hosts can experience data unavailability.

Conditions of occurrence: Reading the allocation map of the virtual volume while running the **`GET_VVMAP`** command.

Impact: High

Customer circumvention: None.

Customer recovery steps: None.

Known Issues

HPE 3PAR OS 3.3.1 MU2 Patch 51 includes the following known issues:

Issue ID: 259760

Issue summary: The external key manager (EKM) rekey operation may not succeed if the process restarts during a rekey operation.

Affected platforms: All StoreServ

Affected software versions: 3.3.1 GA - MU3

Issue description: If the `fivsvr` process restarts during a rekey operation the rekey operation in process will not succeed. Subsequent attempts to rekey may also not succeed. This occurs regardless of the number of EKMs configured for the system.

Symptoms: Rekey operation does not succeed.

An unsuccessful rekey operation should result in the following alert.

```
Task ID# (type "encryption_change", name "Encryption rekey") has failed
(Task Failed). Please see task status for details.
```

A **`showencryption`** command will show a `recovery_needed` state.

Conditions of occurrence: Exit of the `fipsvr` process during rekey operation.

Impact: Low

Customer circumvention: None.

Customer recovery steps: If an Encryption rekey alert is received after a rekey command, verify the encryption state by issuing a **`showencryption`** command.

If the state returned is `recovery_needed`, reissue the rekey command until it is successful.

After a successful rekey operation, the `showencryption` state will be `Normal`.

If the `fivsvr` process exits at any time, it will be automatically restarted.

Affected components

Component	Version
CLI Server	3.3.1.514 (P51)
System Manager	3.3.1.514 (P51)
TPD Kernel Patch	3.3.1.514 (P51)
Persistent Repository	3.3.1.514 (P51)

NOTE: Applying an HPE 3PAR OS patch can cause a restart of the affected OS components. This restart is an expected behavior, which will generate events and alerts. The system continues to serve data, but existing CLI or SSMC sessions could be interrupted.

Verification

The installation of Patch 51 can be verified from an interactive CLI session. Issue the CLI command `showversion -a -b` to verify that Patch 51 is listed:

```
$ showversion -a -b
Release version 3.3.1.410 (MU2)
Patches:  P32,P40,P45,P51

Component Name                   Version
CLI Server                       3.3.1.514 (P51)
CLI Client                       3.3.1.514
System Manager                   3.3.1.514 (P51)
Kernel                           3.3.1.410 (MU2)
TPD Kernel Code                  3.3.1.410 (MU2)
TPD Kernel Patch                 3.3.1.514 (P51)
CIM Server                       3.3.1.410 (MU2)
WSAPI Server                     3.3.1.410 (MU2)
Console Menu                     3.3.1.410 (MU2)
Event Manager                    3.3.1.482 (P45)
Internal Test Tools              3.3.1.410 (MU2)
LD Check Tools                   3.3.1.410 (MU2)
Network Controller               3.3.1.410 (MU2)
Node Disk Scrubber               3.3.1.410 (MU2)
PD Scrubber                      3.3.1.410 (MU2)
Per-Node Server                  3.3.1.482 (P45)
Persistent Repository            3.3.1.514 (P51)
Powerfail Tools                  3.3.1.410 (MU2)
Preserved Data Tools             3.3.1.410 (MU2)
Process Monitor                  3.3.1.410 (MU2)
Software Updater                 3.3.1.467 (P40)
TOC Server                       3.3.1.410 (MU2)
VV Check Tools                   3.3.1.410 (MU2)
Upgrade Check Scripts            181211.U018
File Persona                     1.4.2.40-20171006 (MU2)
SNMP Agent                       1.10.0
SSH                              6.0p1-4+deb7u5
VASA Provider                    3.0.17 (MU2)
Firmware Database                3.3.1.410 (MU2)
Drive Firmware                   3.3.1.410 (MU2)
UEFI BIOS                        05.02.54 (MU2)
MCU Firmware (OKI)               4.8.60 (MU2)
MCU Firmware (STM)               5.3.17 (MU2)
Cage Firmware (DC1)              4.44 (MU2)
Cage Firmware (DC2)              2.64 (MU2)
Cage Firmware (DC3)              08 (MU2)
Cage Firmware (DC4)              2.64 (MU2)
Cage Firmware (DCN1)             4082 (MU2)
Cage Firmware (DCN2)             4082 (MU2)
Cage Firmware (DCS1)             4082 (MU2)
Cage Firmware (DCS2)             4082 (MU2)
Cage Firmware (DCS5)             2.79 (MU2)
Cage Firmware (DCS6)             2.79 (MU2)
Cage Firmware (DCS7)             4082 (MU2)
Cage Firmware (DCS8)             4082 (MU2)
QLogic QLA4052C HBA Firmware     03.00.01.77 (MU2)
QLogic QLE8242 CNA Firmware      04.15.27
QLogic 260x HBA FC Firmware      174.03.70
QLogic 27xx/268x HBA FC Firmware 174.03.70
```

```
QLogic 83xx HBA FCoE Firmware    08.01.05
QLogic 8300 HBA iSCSI Firmware   05.07.35
Emulex LP11002 HBA Firmware      02.82.x10
Emulex LPe12002 HBA Firmware     02.10.x03
Emulex LPe12004 HBA Firmware     02.10.x03
Emulex LPe16002 HBA Firmware     11.1.220.10
Emulex LPe16004 HBA Firmware     11.1.220.10
3PAR FC044X HBA Firmware         200A8
LSI 9201-16e HBA Firmware        17.11.03
LSI 9205-8e HBA Firmware         17.11.03
LSI 9300-8e HBA Firmware         10.10.01
```

NOTE: When displaying the `showversion` command output from the SP, the CLI Client version is static in the SP code and may differ from the output from any other system.

Websites

General websites

Hewlett Packard Enterprise Information Library

www.hpe.com/info/EIL

Single Point of Connectivity Knowledge (SPOCK) Storage compatibility matrix

www.hpe.com/storage/spock

Storage white papers and analyst reports

www.hpe.com/storage/whitepapers

For additional websites, see **Support and other resources**.

Support and other resources

Accessing Hewlett Packard Enterprise Support

- For live assistance, go to the Contact Hewlett Packard Enterprise Worldwide website:

  http://www.hpe.com/assistance

- To access documentation and support services, go to the Hewlett Packard Enterprise Support Center website:

  http://www.hpe.com/support/hpesc

Information to collect

- Technical support registration number (if applicable)
- Product name, model or version, and serial number
- Operating system name and version
- Firmware version
- Error messages
- Product-specific reports and logs
- Add-on products or components
- Third-party products or components

Accessing updates

- Some software products provide a mechanism for accessing software updates through the product interface. Review your product documentation to identify the recommended software update method.
- To download product updates:

  Hewlett Packard Enterprise Support Center

  www.hpe.com/support/hpesc

  Hewlett Packard Enterprise Support Center: Software downloads

  www.hpe.com/support/downloads

  Software Depot

  www.hpe.com/support/softwaredepot

- To subscribe to eNewsletters and alerts:

  www.hpe.com/support/e-updates

- To view and update your entitlements, and to link your contracts and warranties with your profile, go to the Hewlett Packard Enterprise Support Center **More Information on Access to Support Materials** page:

  www.hpe.com/support/AccessToSupportMaterials

IMPORTANT: Access to some updates might require product entitlement when accessed through the Hewlett Packard Enterprise Support Center. You must have an HPE Passport set up with relevant entitlements.

Customer self repair

Hewlett Packard Enterprise customer self repair (CSR) programs allow you to repair your product. If a CSR part needs to be replaced, it will be shipped directly to you so that you can install it at your convenience. Some parts do not qualify for CSR. Your Hewlett Packard Enterprise authorized service provider will determine whether a repair can be accomplished by CSR.

For more information about CSR, contact your local service provider or go to the CSR website:

http://www.hpe.com/support/selfrepair

Remote support

Remote support is available with supported devices as part of your warranty or contractual support agreement. It provides intelligent event diagnosis, and automatic, secure submission of hardware event notifications to Hewlett Packard Enterprise, which will initiate a fast and accurate resolution based on your product's service level. Hewlett Packard Enterprise strongly recommends that you register your device for remote support.

If your product includes additional remote support details, use search to locate that information.

Remote support and Proactive Care information

HPE Get Connected

www.hpe.com/services/getconnected

HPE Proactive Care services

www.hpe.com/services/proactivecare

HPE Proactive Care service: Supported products list

www.hpe.com/services/proactivecaresupportedproducts

HPE Proactive Care advanced service: Supported products list

www.hpe.com/services/proactivecareadvancedsupportedproducts

Proactive Care customer information

Proactive Care central

www.hpe.com/services/proactivecarecentral

Proactive Care service activation

www.hpe.com/services/proactivecarecentralgetstarted

Warranty information

To view the warranty information for your product, see the links provided below:

HPE ProLiant and IA-32 Servers and Options

www.hpe.com/support/ProLiantServers-Warranties

HPE Enterprise and Cloudline Servers

www.hpe.com/support/EnterpriseServers-Warranties

HPE Storage Products

www.hpe.com/support/Storage-Warranties

HPE Networking Products

www.hpe.com/support/Networking-Warranties

Regulatory information

To view the regulatory information for your product, view the *Safety and Compliance Information for Server, Storage, Power, Networking, and Rack Products*, available at the Hewlett Packard Enterprise Support Center:

www.hpe.com/support/Safety-Compliance-EnterpriseProducts

Additional regulatory information

Hewlett Packard Enterprise is committed to providing our customers with information about the chemical substances in our products as needed to comply with legal requirements such as REACH (Regulation EC No 1907/2006 of the European Parliament and the Council). A chemical information report for this product can be found at:

www.hpe.com/info/reach

For Hewlett Packard Enterprise product environmental and safety information and compliance data, including RoHS and REACH, see:

www.hpe.com/info/ecodata

For Hewlett Packard Enterprise environmental information, including company programs, product recycling, and energy efficiency, see:

www.hpe.com/info/environment

Documentation feedback

Hewlett Packard Enterprise is committed to providing documentation that meets your needs. To help us improve the documentation, send any errors, suggestions, or comments to Documentation Feedback (**docsfeedback@hpe.com**). When submitting your feedback, include the document title, part number, edition, and publication date located on the front cover of the document. For online help content, include the product name, product version, help edition, and publication date located on the legal notices page.